(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08335207 A**

(43) Date of publication of application: **17 . 12 . 96**

(51) Int. Cl **G06F 15/00**
G09C 1/00
H04L 9/00
H04L 9/10
H04L 9/12
H04L 9/32

(21) Application number: **07140291**

(22) Date of filing: **07 . 06 . 95**

(71) Applicant: **HITACHI LTD**

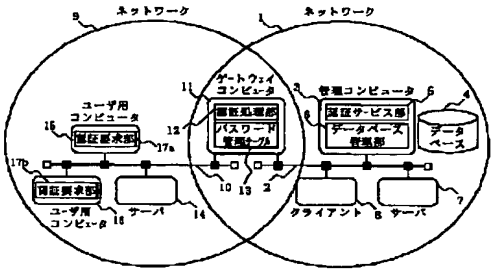
(72) Inventor: **ARAI MASATO**
ITO HIROMICHI
ITOU HISAYA

(54) **AUTHORIZING METHOD FOR NETWORK USER**

(57) Abstract:

PURPOSE: To exclude an illegal gateway computer by ciphering a cipher key with another cipher key by an administration computer before a log-in processing for a user and then distributing the ciphered key.

CONSTITUTION: The user of a network 1 sends an authorization request and his user ID to the administration computer 3 when logging in the network 1. The administration computer 3 when receiving them returns a log-in certificate ciphered with the password of the user and the cipher key to the client 8 that the user uses. On the side of the client 8, the log-in certificate and cipher key are ciphered with the password that the user inputs. Consequently, when the user inputs the correct password at the time of logging-in operation, the user can obtain the log-in certificate and cipher key and utilize resources of the network 1 thereafter by using them. An illegal user who knows no password, on the other hand, can decipher no log-in certificate and cipher key and is unable to use the resources of the network 1.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－335207

(43)公開日　平成８年(1996)12月17日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０	9364－5L	Ｇ０６Ｆ	15/00	３３０Ａ
Ｇ０９Ｃ	1/00		7259－5Ｊ	Ｇ０９Ｃ	1/00	
Ｈ０４Ｌ	9/00			Ｈ０４Ｌ	9/00	Ｚ
	9/10					Ａ
	9/12					

審査請求　未請求　請求項の数６　ＯＬ　（全 ９ 頁）　最終頁に続く

(21)出願番号　特願平7－140291

(22)出願日　平成７年(1995)６月７日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　荒井　正人
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　伊藤　浩道
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　伊藤　寿哉
神奈川県横浜市戸塚区戸塚町5030番地株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　小川　勝男

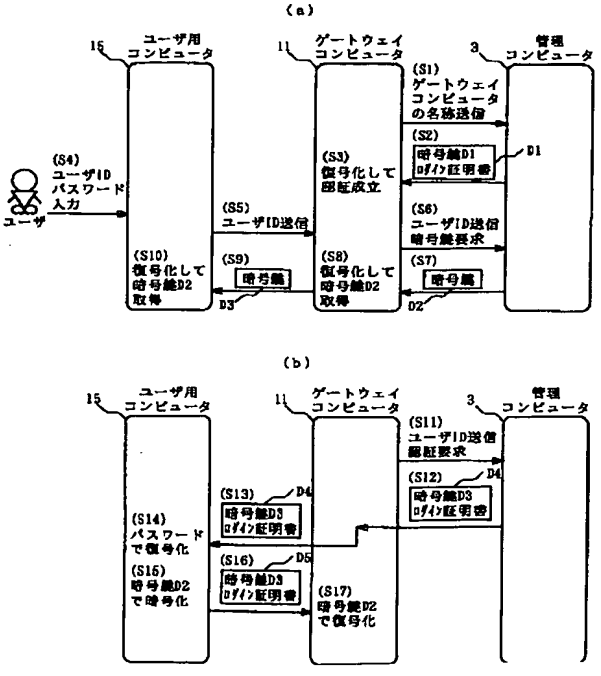
(54)【発明の名称】　ネットワークユーザ認証方法

(57)【要約】

【構成】ユーザ認証手段を有する管理計算機とユーザ用計算機とを、ゲートウェイ計算機を介して接続し、ユーザ用計算機から、管理計算機にログインする場合、先ず管理計算機がゲートウェイ計算機とユーザ用計算機のみに共通の暗号鍵Ｄ２を配布する（Ｓ１～Ｓ１０）。暗号鍵Ｄ２はそれぞれ正当なゲートウェイ計算機とユーザだけが知っている鍵により暗号化された形で渡される。次に、管理計算機がユーザのパスワードで暗号化されたログイン証明書Ｄ４を作成し、ゲートウェイ計算機を介してユーザ用計算機に送信する（Ｓ１）。ユーザが入力したパスワードでこれを復号化し（Ｓ１４）、ゲートウェイ計算機に送信する。

【効果】パスワードを通信媒体上に流さずに他のネットワークへログインでき、不正なゲートウェイ計算機を排除でき、セキュリティの点で優れた統合ネットワークの利用ができる。

図２



1

【特許請求の範囲】

【請求項１】ユーザおよびコンピュータの名称やパスワードなどの情報を管理するデータベースを有する管理コンピュータと、ユーザが操作するためのユーザ用コンピュータと、前記ユーザ用コンピュータから前記管理コンピュータへのゲートウェイとなるゲートウェイコンピュータとが、通信媒体を介して物理的・論理的に接続されたコンピュータネットワークシステムのネットワークユーザ認証方法であって、前記ゲートウェイコンピュータは、前記データベースに登録されており、前記ゲートウェイコンピュータの名称を前記管理コンピュータに送信するプロセスと、前記ゲートウェイコンピュータから送られた名称に基づいて、前記管理コンピュータが、前記データベースを検索し、前記名称が登録されている場合は、認証に必要なログイン証明書と暗号鍵Ｄ１を作成して前記ゲートウェイコンピュータのパスワードにより暗号化し、前記ゲートウェイコンピュータに送信するプロセスと、前記ゲートウェイコンピュータが、暗号化された前記ログイン証明書と暗号鍵Ｄ１を自己のパスワードによって復号化するプロセスと、ユーザが前記ネットワークの利用を開始する際に、ユーザ用コンピュータから入力したユーザ名を前記ゲートウェイコンピュータに送信するプロセスと、前記ゲートウェイコンピュータが、前記ユーザ名を前記管理コンピュータに送信するプロセスと、前記ゲートウェイコンピュータから送られたユーザ名に基づいて、前記管理コンピュータが、前記データベースを検索し、前記ユーザ名が登録されている場合は、認証に必要なログイン証明書と暗号鍵Ｄ３を作成して前記ユーザのパスワードにより暗号化し、前記ゲートウェイコンピュータに送信するプロセスと、暗号化された前記ログイン証明書と暗号鍵Ｄ３を、前記ゲートウェイコンピュータが前記ユーザ用コンピュータに送信するプロセスと、前記ユーザ用コンピュータと、前記ゲートウェイコンピュータは共通の暗号鍵Ｄ２を所有しており、前記ユーザ用コンピュータが、前記ユーザが入力したパスワードにより前記ログイン証明書と暗号鍵Ｄ３を復号化し、復号できたか否かによって前記ユーザの認証を行い、復号された前記ログイン証明書と暗号鍵Ｄ３を、前記暗号鍵Ｄ２で暗号化して、前記ゲートウェイコンピュータに送信するプロセスと、前記ゲートウェイコンピュータが、前記ログイン証明書と暗号鍵Ｄ３を、暗号鍵Ｄ２で復号化して所有するプロセスを備えることを特徴とするネットワークユーザ認証方法。

【請求項２】請求項１において、前記管理コンピュータが、暗号鍵Ｄ２と、暗号鍵Ｄ２をユーザのパスワードで暗号化したものとを併せて暗号鍵Ｄ１で暗号化したデータを、前記ゲートウェイコンピュータに送信するプロセスと、

前記ゲートウェイコンピュータが、暗号鍵Ｄ１によりデータを復号化することにより暗号鍵Ｄ２を取得し、前記

2

ユーザのパスワードで暗号化した暗号鍵Ｄ２を前記ユーザ用コンピュータに送信するプロセスと、

前記ユーザ用コンピュータが、ユーザの入力したパスワードで復号化して暗号鍵Ｄ２を取得するプロセスを備えることで、

身元の正しいユーザおよびゲートウェイコンピュータのみが共通の暗号鍵Ｄ２を取得できるネットワークユーザ認証方法。

【請求項３】請求項１または請求項２において、前記ユーザ用コンピュータから、前記暗号鍵Ｄ２によりゲートウェイコンピュータの正当性を確認し、パスワードを通信媒体上に流さずに、前記管理コンピュータによる認証処理を行うネットワークユーザ認証方法。

【請求項４】請求項１に記載の前記管理コンピュータと、ファイル操作など各種処理を依頼する役割を持つ一つ以上のクライアントと、前記クライアントからの依頼を受けて処理を実行する役割を持つ一つ以上の第一サーバとを、第一の通信媒体に物理的・論理的に接続して構成されたネットワーク１と、

前記ユーザ用コンピュータと、前記ユーザ用コンピュータからの依頼を受けて処理を実行する役割を持つ一つ以上の第二のサーバとを、第二の通信媒体に物理的・論理的に接続して構成されたネットワーク９を前記ゲートウェイコンピュータを介して接続した統合ネットワーク。

【請求項５】請求項１に記載の前記管理コンピュータと、ファイル操作など各種処理を依頼する役割を持つ一つ以上の第一クライアントと、前記第一クライアントからの依頼を受けて処理を実行する役割を持つ一つ以上の第一サーバとを、第一の通信媒体に物理的・論理的に接続して構成されたネットワーク１と、ファイル操作など各種処理を依頼する役割を持つ一つ以上の第二クライアントと、前記第二クライアントからの依頼を受けて処理を実行する役割と、前記ユーザ用コンピュータと同じ役割を持つ一つ以上の第二サーバとを、第二の通信媒体に物理的・論理的に接続して構成されたネットワーク９を、前記ゲートウェイコンピュータを介して接続し、前記第二サーバは、ネットワーク９とネットワーク１におけるユーザの名称とパスワードの対応付けを管理するパスワード管理テーブルと、ネットワーク９のユーザを認証する認証手段とを有し、前記認証手段により認証されたユーザについて、前記パスワード管理テーブルから、ネットワーク１におけるユーザの名称とパスワードを取り出して、ネットワーク１への認証処理を行うよう構成された統合ネットワーク。

【請求項６】請求項４または請求項５において、ユーザが同時に異なる複数のネットワークへ認証されるように作用するネットワークユーザ認証方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はネットワークユーザ認証

方法に関する。

【０００２】

【従来の技術】近年、サービスを提供する機能を持つコンピュータと、これらにサービスを依頼する機能を持つコンピュータを相互に接続することで処理の分業化を図るコンピュータネットワークが企業などに導入されてきている。この方式は、処理依頼とサービス提供という観点からクライアント・サーバモデルと呼ばれる。

【０００３】今後更にコンピュータネットワークが普及するにつれて、多種多様なネットワークが共存し、それらを相互に接続することにより各ネットワークの資源を利用する統合ネットワークの必要性が高まることが予想される。

【０００４】統合ネットワークの形態の一つとして、図１に示すようにゲートウェイコンピュータを介して各ネットワークを相互にアクセスするものがある。このような統合ネットワークの資源を利用するために、ユーザは接続された各ネットワーク中のユーザ認証機能を有するサーバに対して自分の身元の正当性を証明する必要がある。この動作をログインと呼ぶ。多くの場合、ユーザはサーバに対してパスワードを提供することにより自分の身元を証明する。

【０００５】図１において、ユーザはネットワーク９のユーザ用コンピュータ１５～１６からネットワーク１へログインする際に、ゲートウェイコンピュータ１１を介することとなる。このような２階層以上のネットワークにおけるセキュリティに関する発明は、特開平２－１６６６９号公報の「セキュリティ方式」がある。「セキュリティ方式」は、ユーザが入力した各ノードへのパスワードを、直接のアクセス先となるノード（本発明におけるゲートウェイコンピュータに相当する）に送信し、ノードがパスワードをチェックすることで他のノードへのアクセス権の有無を判断する方式である。

【０００６】また、ネットワークログインの方式は、特開平５－３５６７８号公報の「ユーザ認証方式」のように、パスワードの機密性を高めるために、パスワードを通信媒体上に流さずにログイン可能とする方式がある。

【０００７】

【発明が解決しようとする課題】このように、ゲートウェイコンピュータを介して各ネットワークの資源にアクセスする統合ネットワークにおいて、ユーザはネットワークの資源を利用する前に、必ずゲートウェイコンピュータを介して他のネットワークへログインすることとなる。このとき、ゲートウェイコンピュータが悪意をもったユーザにより仕組まれたものである場合、ゲートウェイコンピュータによって他のユーザのパスワードが盗まれたり、データが破壊される危険がある。しかし、「セキュリティ方式」はパスワードの送信先となるノード（本発明におけるゲートウェイコンピュータに相当する）の正当性をチェックする手段がないため、不正なノードを除外できないという問題がある。

【０００８】更に、図１におけるネットワーク１が「ユーザ認証方式」のようにパスワードを通信媒体上に送信せずにログイン可能とするネットワークであるとする。この場合、ネットワーク１のセキュリティレベルを保持するためには、ユーザがネットワーク９からゲートウェイコンピュータを介してネットワーク１にログインする際にもパスワードを送信しないことが望ましい。しかし、「ユーザ認証方式」では、他のネットワークからゲートウェイコンピュータを介してログインする場合のパスワード機密保持については記述されていない。

【０００９】本発明の目的は、ゲートウェイコンピュータを介して各ネットワークの資源にアクセスする統合ネットワークにおいて、先ずゲートウェイコンピュータの正当性を確認した上で、ユーザのパスワードを通信媒体上に流さずに他のネットワークへログインする方式を提供することにある。

【００１０】

【課題を解決するための手段および作用】本発明は、ゲートウェイコンピュータを介して、ユーザが使用するユーザ用コンピュータと、ネットワーク内のコンピュータやユーザの名称およびパスワードが登録されたデータベースを有する管理コンピュータとを接続した統合ネットワークにおいて、ゲートウェイコンピュータは自己のパスワードを登録したパスワード管理テーブルを有しており、ユーザがログインする前にゲートウェイコンピュータが管理コンピュータから暗号鍵Ｄ１をゲートウェイコンピュータのパスワードで暗号化された形で取得するプロセスと、ゲートウェイコンピュータが自己のパスワードをパスワード管理テーブルから読み出して暗号鍵Ｄ１を復号化するプロセスと、ユーザがログイン要求を出したときに管理コンピュータが暗号鍵Ｄ２を暗号鍵Ｄ１で暗号化したデータと、暗号鍵Ｄ２をユーザのパスワードで暗号化したデータをゲートウェイコンピュータに配布するプロセスと、ゲートウェイコンピュータが暗号鍵Ｄ１で暗号化された暗号鍵Ｄ２を復号化すると共に、ユーザのパスワードで暗号化された暗号鍵Ｄ２をユーザが使用するユーザ用コンピュータに配布するプロセスと、ユーザ用コンピュータがユーザの入力したパスワードで暗号鍵Ｄ２を復号化するプロセスによりゲートウェイコンピュータとユーザ用コンピュータに共通の暗号鍵Ｄ２を配布し、次にゲートウェイコンピュータが管理コンピュータに対してユーザのログイン要求を提示するプロセスと、管理コンピュータがデータベースを検索し、ユーザ名が登録されている場合は、認証に必要なログイン証明書と暗号鍵Ｄ３を作成してユーザのパスワードにより暗号化し、ゲートウェイコンピュータに送信するプロセスと、暗号化されたログイン証明書と暗号鍵Ｄ３を、ゲートウェイコンピュータがユーザ用コンピュータに送信するプロセスと、ユーザ用コンピュータがユーザの入力し

たパスワードによりログイン証明書と暗号鍵Ｄ３を復号化するプロセスと、ログイン証明書と暗号鍵Ｄ３を暗号鍵Ｄ２により暗号化してゲートウェイコンピュータに送信するプロセスと、ゲートウェイコンピュータが暗号鍵Ｄ２によりログイン証明書と暗号鍵Ｄ３を復号化するプロセスを具備することを特徴とするネットワークユーザ認証方法である。

【００１１】本発明のネットワークユーザ認証方法では、ユーザのログイン処理の前に、管理コンピュータが暗号鍵Ｄ２を暗号鍵Ｄ１で暗号化してからゲートウェイコンピュータに配布するので、正当なゲートウェイコンピュータのみが暗号鍵Ｄ２を復号化できる。一方、ユーザ用コンピュータには暗号鍵Ｄ２をユーザのパスワードで暗号化した形で配布するので、正当なユーザのみが暗号鍵Ｄ２を復号化できる。

【００１２】次に、管理コンピュータから配布されたログイン証明書と暗号鍵Ｄ３を、ユーザ用コンピュータでユーザが入力したパスワードで復号化することで、ユーザのパスワードがネットワークの回線を流れることはない。また、復号化したログイン証明書と暗号鍵Ｄ３は、ユーザ用コンピュータにおいて暗号鍵Ｄ２により暗号化されてゲートウェイコンピュータに送信されるため、暗号鍵Ｄ２を知らない第三者に盗まれる危険がない。

【００１３】

【実施例】以下、本発明の実施例を図面を参照しながら説明する。図１は本発明の一実施例として、互いに独立に管理される二つのネットワーク環境を、ゲートウェイコンピュータ１１を用いて接続する場合の構成例を示す図である。

【００１４】図１において、後述する各要素で構成されるネットワーク１、ネットワーク２を構成する各要素（後述）間を物理的・論理的に接続し、各種データ転送の媒体となる通信媒体、３はネットワーク１を構成する各要素やユーザの認証処理を専門に行う管理コンピュータ、４はネットワーク１の各要素やユーザに関する情報（ＩＤ、パスワード等）を管理するためのデータベース、５はネットワークの各要素やユーザからの要求に応じて、暗号鍵やログイン証明書を要求元に与える認証サービス部、６はデータベースからデータの読み出しや書き込みを行うデータベース管理部、７はクライアント８からの要求に応じて各種サービスを提供するサーバ、８はネットワーク１のユーザにコマンドインタフェースやアプリケーションプログラムを提供し、それらを通じてユーザから発せられる要求に応じて、管理コンピュータやサーバ７と通信を行うクライアント、９はネットワーク１とは独立に管理され、後述する各要素で構成されるネットワーク９、１０はネットワーク９内の後述する各要素間を物理的・論理的に接続し、各種データ転送の媒体となる通信媒体、１１は通信媒体２および通信媒体１０に接続され、後述するユーザ用コンピュータ１５～１６からのコマンドをネットワーク１に送信し、結果をユーザ用コンピュータに返送する役割をもつゲートウェイコンピュータ、１２は管理コンピュータに認証要求を送信してネットワーク１へのログイン処理を行う認証処理部、１３はゲートウェイコンピュータおよびネットワーク９のユーザに関する情報（ＩＤやパスワード等）を管理するパスワード管理テーブル、１４は後述するユーザ用コンピュータ１５～１６からの要求に応じて各種サービスを提供するサーバ、１５～１６はネットワーク９のユーザにコマンドインタフェースやアプリケーションプログラムを提供し、それらを通じてユーザから発せられる要求に応じて、ゲートウェイコンピュータ１１やサーバ１４と通信を行うユーザ用コンピュータであり、それぞれユーザのＩＤやパスワードを入力する認証要求部１７ａと１７ｂを備えている。

【００１５】ネットワーク１及びネットワーク９は、それぞれ単独での運用が可能になっている。単独の運用での動作を簡単に説明する。

【００１６】複数のコンピュータが接続され、各々のコンピュータが管理する資源を、他のコンピュータからも利用できるように構成されたネットワークシステムでは、ユーザはネットワークの資源を利用する前に自分の身元を証明するためのログイン動作を行わなければならない。一般的にログインとは、ユーザＩＤと呼ばれるユーザの識別子と、パスワードなどユーザ本人のみが持つ情報を示すことで、ネットワークシステムに対して自分が正規のネットワークユーザであることを証明するための手続き（これを認証という）である。

【００１７】本実施例におけるネットワーク１は、ネットワーク内にユーザ認証処理を専門とする管理コンピュータ３を有している。ネットワーク１のすべてのユーザは、ログイン時にこの管理コンピュータ３に対して認証要求とユーザＩＤを送信する。管理コンピュータ３はログイン要求を受けると、ユーザのパスワードで暗号化したログイン証明書と暗号鍵をユーザが使用するクライアントに返す。ログイン証明書は、ユーザがネットワーク１の資源を利用する際に、自分の身元を証明するために必要なものである。一方、暗号鍵は管理コンピュータ３と送受信するデータを暗号化復号化するために必要なものである。クライアント側では、ユーザが入力したパスワードによりこのログイン証明書と暗号鍵を復号化する。つまり、ユーザが正しいパスワードを入力すればログイン証明書と暗号鍵を入手でき、以後ユーザはそれらを用いてネットワーク１の資源を利用できるようになる。反対にパスワードを知らない不正なユーザはログイン証明書と暗号鍵を復号化できないため、ネットワーク１の資源を利用できないことになる。以上のようにネットワーク１では、ログイン時にユーザのパスワードが通信媒体２に流れないという特徴がある。

【００１８】一方、本実施例におけるネットワーク９で

は、ネットワーク内の全てのサーバがユーザ認証手段とユーザの暗号化されたパスワードを管理する手段を有している。ログイン時には、例えばユーザ用コンピュータ１５ではユーザが入力したパスワードを暗号化して、ユーザＩＤと併せてサーバに送信する。このときパスワードの暗号化に使用する鍵は常に固定なものとする。サーバはクセイアントから受信したユーザの暗号化パスワードを、サーバ自身が管理する暗号化パスワードと照合する。両者が一致していれば、サーバが管理するネットワークの資源に対してアクセスを許可する。反対に、両者が一致しなければアクセスを許可しない。

【００１９】図２の（ａ）と（ｂ）は、ネットワーク１に登録されているユーザが、本発明のネットワークユーザ認証方法により、ユーザ用コンピュータ１５からネットワーク１にログインする処理を示したものである。図２（ａ）は、ユーザのログイン処理に先立ってユーザ用コンピュータ１５からゲートウェイコンピュータ１１の正当性を確認するための手順を示している。同図に示すように、

（Ｓ１）ゲートウェイコンピュータの認証処理部１２は、起動時にゲートウェイコンピュータ自身の名称を管理コンピュータ３に送信し、認証要求を出す。

【００２０】（Ｓ２）管理コンピュータ３は、暗号鍵１とログイン証明書を作成し、これをゲートウェイコンピュータのパスワードで暗号化したデータＤ１を送信する。データＤ１の構造を図３（ａ）に示す。図３において、３１は暗号鍵であり、３２はログイン証明書である。３３は暗号鍵３１とログイン証明書３２を認証要求元であるゲートウェイコンピュータのパスワードで暗号化していることを表す。また、ゲートウェイコンピュータのパスワードは、データベース４で管理されており、認証サービス部５がデータベース管理部６を通じて読み出す。図４に、データベース４で管理される情報の一例を示す。管理コンピュータ３は、例えば、立ち入り制限のある安全な部屋に配置され、ネットワーク１の管理者のみがデータベース４をアクセス可能とすることで、パスワードの機密保護を行う。

【００２１】（Ｓ３）認証処理部１２は、パスワード管理テーブル１３からゲートウェイコンピュータのパスワードを取り出してデータＤ１を復号化し、ログイン証明書と暗号鍵をパスワード管理テーブル１３に登録する。これにより、正当なゲートウェイコンピュータだけが暗号鍵とログイン証明書を取得でき、管理コンピュータにより認証されたこととなる。図５にパスワード管理テーブ１３で管理される情報の一例を示す。同図に示すように、パスワード管理テーブル１３には、ネットワーク１におけるユーザ及びゲートウェイコンピュータ自身のＩＤとパスワードの他に、ネットワーク１におけるログイン証明書と暗号鍵が登録されている。ログイン証明書と暗号鍵は、ネットワーク１にログインしている間のみ登録される。また、パスワード管理テーブル１３は、ネットワーク９の管理者のみがアクセス可能とすることで、パスワードやログイン証明書および暗号鍵の機密保護を行う。

【００２２】（Ｓ４）ユーザは、認証要求部１７ａからユーザＩＤとパスワードを入力する。

【００２３】（Ｓ５）認証要求部１７ａは、ゲートウェイコンピュータにユーザＩＤを送信する。

【００２４】（Ｓ６）認証処理部１２は、管理コンピュータにユーザＩＤを送信し、ユーザ用コンピュータ１５とゲートウェイコンピュータ１１との間で使う暗号鍵を要求する。

【００２５】（Ｓ７）認証サービス部５は暗号機２を作成し、ゲートウェイコンピュータに送信する。このとき、送信データＤ２は図３（ｂ）に示すような構造になっている。図３（ｂ）において、３４は暗号鍵Ｄ２であり、３５は暗号鍵Ｄ２をユーザのパスワードで暗号化したデータである。また、３６は暗号鍵３４と３５のデータを暗号鍵で暗号化したデータを表す。

【００２６】（Ｓ８）認証処理部１２は、（Ｓ３）で取得した暗号鍵Ｄ１によりデータＤ２を復号化し、暗号鍵Ｄ２とデータＤ３を取得する。データＤ３は図３（ｂ）における３５のデータに相当する。このとき、ゲートウェイコンピュータが暗号鍵Ｄ１を知らなければ暗号鍵Ｄ２とデータＤ３は取得できない。言い換えれば、暗号鍵Ｄ２とデータＤ３を取得したことは、管理コンピュータ３によって認証されていることを意味する。

【００２７】（Ｓ９）認証処理部１２は、データＤ３をユーザ用コンピュータ１５へ送信する。

【００２８】（Ｓ１０）認証要求部１７ａは、データＤ３をユーザが入力したパスワードで復号化し、暗号鍵Ｄ２を取得する。ここで、ユーザのパスワードを知っているのは、ユーザ本人と管理コンピュータだけである。つまり、データＤ３を作成したのは管理コンピュータであり、不正なゲートウェイコンピュータが偽造することはあり得ない。また、ゲートウェイコンピュータが管理コンピュータからデータＤ３を取得するには暗号鍵１を必要とする。ゲートウェイコンピュータが暗号鍵１を所有していることは、管理コンピュータ３により認証されている、つまり正当なゲートウェイコンピュータであることが証明される。

【００２９】以上により、正当なゲートウェイコンピュータとユーザ用コンピュータ１５のみに共通の暗号鍵２が配布される。以後、暗号鍵２によって暗号化されたデータを交換することにより、ユーザ用コンピュータ１５とゲートウェイコンピュータ１１が互いの正当性を確認できる。

【００３０】次に図２（ｂ）は、ゲートウェイコンピュータ１１が正当なものであることを確認した上で、ユーザがネットワーク１へログインするまでの手順を示して

いる。

【００３１】同図に示すように、

（Ｓ１１）認証処理部１２は、ユーザＩＤを送信して、ユーザ認証を要求する。

【００３２】（Ｓ１２）認証サービス部５は、暗号鍵Ｄ３とログイン証明書を作成し、これをユーザのパスワードで暗号化したデータＤ４を送信する。データＤ４の構造は、前述の図３（ａ）と同じである。また、ユーザのパスワードは、データベース４で管理されており、認証サービス部５がデータベース管理部６を通じて読み出す。

【００３３】（Ｓ１３）認証処理部１２は、データＤ４をそのままの状態でユーザ用コンピュータに送信する。

【００３４】（Ｓ１４）認証要求部１７ａは、データＤ４をユーザのパスワードで復号化し、暗号鍵３とログイン証明書を取得する。

【００３５】ここで、本発明のネットワークユーザ認証方法では、ネットワーク１の各資源に直接アクセスするのはユーザ用コンピュータ１５ではなくゲートウェイコンピュータ１１である。したがって、ネットワーク１の資源にアセスするために必要なログイン証明書と暗号鍵３をゲートウェイコンピュータ１１に渡す必要がある。このとき、ログイン証明書と暗号鍵３が第三者によって盗まれないためには暗号化する必要がある。そこで暗号化の鍵として、（Ｓ１）～（Ｓ１０）で取得した暗号鍵２を使用することにした。以下（Ｓ１５）～（Ｓ１７）にその処理を示す。

【００３６】（Ｓ１５）認証要求部１７ａは、暗号鍵Ｄ３とログイン証明書を（Ｓ１０）で取得した暗号鍵Ｄ２で暗号化する。これをデータＤ５とする。

【００３７】（Ｓ１６）認証要求部１７ａは、データＤ５をゲートウェイコンピュータ１１へ送信する。

【００３８】（Ｓ１７）認証処理部１２は、データＤ５を暗号鍵Ｄ２で復号化し、暗号鍵Ｄ３とログイン証明書をパスワード管理テーブル１３に登録する。ここで、暗号鍵Ｄ２を所有しているのは、ユーザ用コンピュータとゲートウェイコンピュータだけであるため、不正なコンピュータがデータＤ５を盗んでも復号化できない。

【００３９】以上により、ネットワーク１へのログインが完了する。以後、ユーザがゲートウェイコンピュータを介してネットワーク１の資源へアクセスする場合、ゲートウェイコンピュータがユーザのログイン証明書をパスワード管理テーブル１３から取り出して利用することとなる。

【００４０】なお、上記の説明において、ゲートウェイコンピュータ１１とサーバ１４は別々のコンピュータであるが、両者は１台のコンピュータであっても良い。更にパスワード管理テーブル１３において、図６に示すようなネットワーク１とネットワーク９におけるユーザのＩＤおよびパスワードの対応付けを管理し、ユーザがサーバ１４にログインすると認証処理部１２がパスワード管理テーブル１３からユーザのＩＤとパスワードを取り出してネットワーク１へのログイン処理を実行するよう構成する。これにより、サーバ１４とネットワーク１の両方にログインする場合でも、ユーザはサーバ１４へのログイン操作だけで、ネットワーク１にもログインできる。ただし、ネットワーク１へのログインについては、ユーザが選択可能であってもよい。

【００４１】また、同じくゲートウェイコンピュータ１１とサーバ１４を１台のコンピュータとした場合の例として、ゲートウェイコンピュータ１１から管理コンピュータ５へのアクセスは、常にクライアント８を介して行うこととし、図２におけるゲートウェイコンピュータ１１の処理をクライアント８が行い、ユーザ用コンピュータ１５の処理をゲートウェイコンピュータ１１が行うように構成しても良い。ネットワーク１におけるユーザのパスワードは、ゲートウェイコンピュータ１１が図６に示すパスワード管理テーブルから読み出して使用する。この場合、実施例と同様にして不正なクライアント８を排除することができる。

【００４２】他のシステム構成として、ゲートウェイコンピュータ１１とクライアント８は１台のコンピュータであっても良い。また、ゲートウェイコンピュータ１１とクライアント８およびサーバ１４が１台のコンピュータであっても良い。

【００４３】

【発明の効果】本発明は、各々独立に管理されるネットワークをゲートウェイコンピュータを介して相互に接続したネットワークシステムにおいて、不正なゲートウェイコンピュータを排除し、且つパスワードを通信媒体上に流さずにログインできるので、ユーザは各ネットワークのセキュリティレベルを損なうことなく、複数のネットワークの資源を利用することができる。

【００４４】また本発明は、ユーザが一度の操作で複数のネットワークへログインできるので、複数のネットワークの資源を利用する場合でもユーザにとってログイン操作の負担が増えない。

【図面の簡単な説明】

【図１】本発明の実施例の統合ネットワークシステムのブロック図。

【図２】本発明の実施例の処理シーケンスを示す説明図。

【図３】図２における送信データの説明図。

【図４】図１におけるデータベース４に記録されるデータの例を示す説明図。

【図５】図１におけるパスワード管理テーブル１３に記録されるデータの例を示す説明図。

【図６】本発明の実施例のパスワード管理テーブルに記録されるデータの一例を示す説明図。

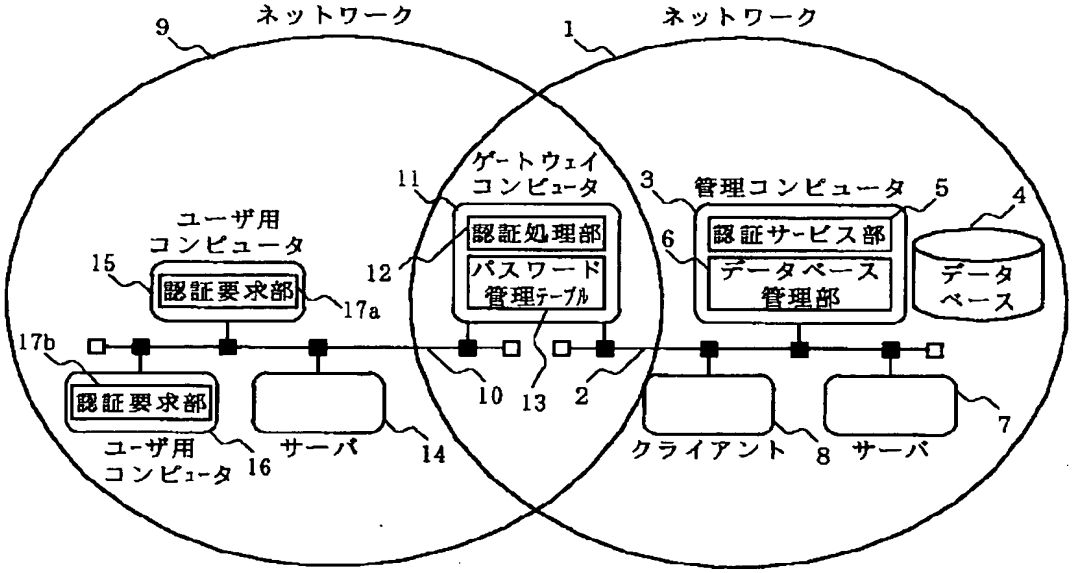
【符号の説明】

11　　12

３…管理コンピュータ、
１１…ゲートウェイコンピュータ、
＊１５…ユーザ用コンピュータ。
＊

【図１】

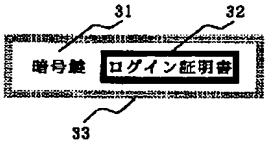
図１



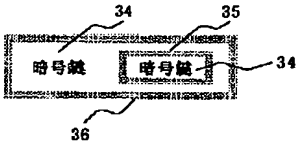
【図３】

図３

(a)



(b)



【図４】

図４

4

ＩＤ	Ｐａｓｓｗｏｒｄ
ＧＷ＿０１	ａａａａ
ｕｓｅｒ＿Ａ	ｘｘｘ
ｕｓｅｒ＿Ｂ	ｙｙｙ
ｕｓｅｒ＿Ｃ	ｗｗｗ
・・・	

【図５】

図５

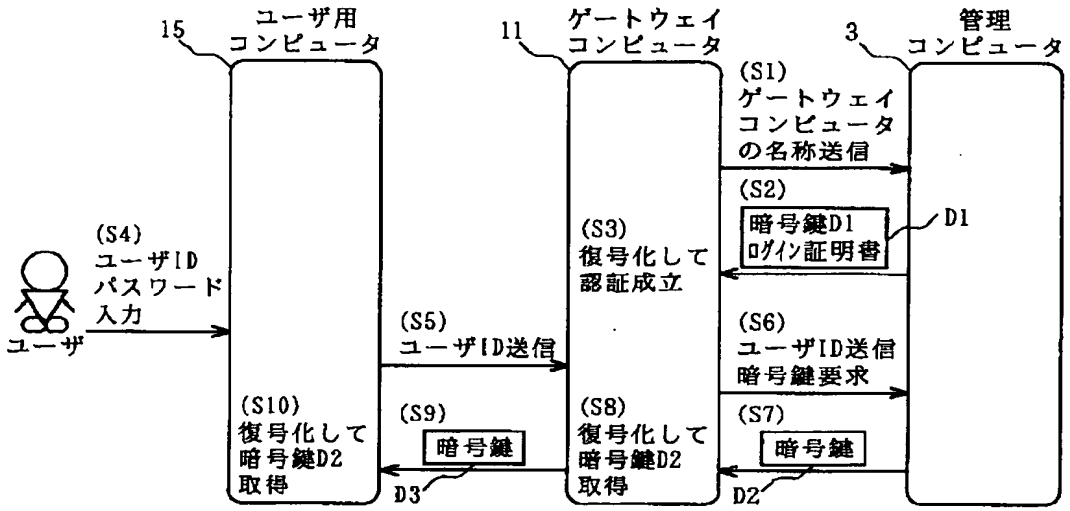
13

ﾈｯﾄﾜｰｸ１のＩＤ	ﾈｯﾄﾜｰｸ１のPassword	ログイン証明書	暗号鍵
ＧＷ＿０１	ａａａａ	８０００ｈ	６０００ｈ
ｕｓｅｒ＿Ａ	――	８０３２ｈ	６００８ｈ
ｕｓｅｒ＿Ｂ	――	８０６４ｈ	６０１６ｈ
ｕｓｅｒ＿Ｃ	――	８０９６ｈ	６０２４ｈ
・・・	・・・	・・・	・・・

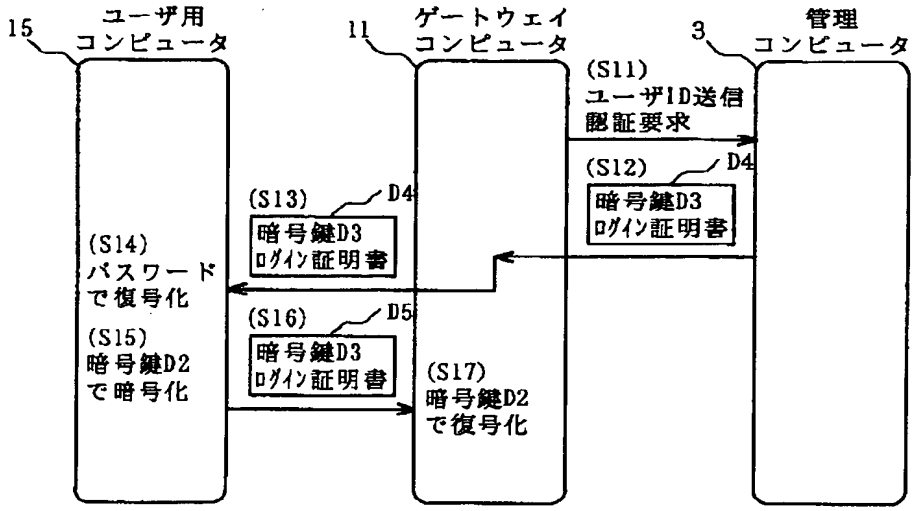
【図２】

図２

（ａ）


15
ユーザ用
コンピュータ
11
ゲートウェイ
コンピュータ
3
管理
コンピュータ
(S1)
ゲートウェイ
コンピュータ
の名称送信
(S2)
暗号鍵D1
ログイン証明書
D1
(S3)
復号化して
認証成立
(S4)
ユーザID
パスワード
入力
ユーザ
(S5)
ユーザID送信
(S6)
ユーザID送信
暗号鍵要求
(S7)
暗号鍵
D2
(S8)
復号化して
暗号鍵D2
取得
(S9)
暗号鍵
D3
(S10)
復号化して
暗号鍵D2
取得

（ｂ）


15
ユーザ用
コンピュータ
11
ゲートウェイ
コンピュータ
3
管理
コンピュータ
(S11)
ユーザID送信
認証要求
(S12)
D4
暗号鍵D3
ログイン証明書
(S13)
D4
暗号鍵D3
ログイン証明書
(S14)
パスワード
で復号化
(S15)
暗号鍵D2
で暗号化
(S16)
D5
暗号鍵D3
ログイン証明書
(S17)
暗号鍵D2
で復号化

【図６】

図６

13a

ネットワーク2のID	ネットワーク2のPassword	ネットワーク1のID	ネットワーク1のPassword	ログイン証明書	暗号鍵
——	——	GW_01	aaaa	８０００ｈ	６０００ｈ
USER_1	XXX	user_A	xxx	８０３２ｈ	６００８ｈ
USER_2	YYY	user_B	yyy	——	——
USER_3	ZZZ	user_C	zzz	８０９６ｈ	６０２４ｈ
・・・	・・・	・・・	・・・	・・・	・・・

フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/32				